

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

ЛАБОРАТОРНАЯ РАБОТА №1:
«Мониторинг событий информационной безопасности»

Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

Москва, 2022 г.

Часть 1. SAN-сети

Сеть хранения данных (англ. Storage Area Network, SAN) представляет собой архитектурное решение для подключения внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические приводы к серверам таким образом, чтобы операционная система распознала подключенные ресурсы как локальные.

SAN характеризуются предоставлением так называемых сетевых блочных устройств (обычно посредством протоколов Fibre Channel, iSCSI или AoE), в то время как сетевые хранилища данных (англ. Network Attached Storage, NAS) нацелены на предоставление доступа к хранящимся на их файловой системе данным при помощи сетевой файловой системы (такой как NFS, SMB/CIFS, или Apple Filing Protocol). При этом категоричное разделение SAN и NAS является искусственным: с появлением iSCSI началось взаимное проникновение технологий с целью повышения гибкости и удобства их применения (например, в 2003 году NetApp уже предоставляли iSCSI на своих NAS, а EMC и HDS — наоборот, предлагали NAS-шлюзы для своих SAN-массивов).

Уровни угроз

Риск всегда начинается с угрозы. Угрозы можно разделить на три основных уровня. Первый уровень угроз является непреднамеренным и обусловлен несчастными случаями или ошибками. Хотя эти угрозы не являются преднамеренными, они распространены и могут привести к простоям и потере доходов. Второй уровень угроз - это простые вредоносные атаки, использующие существующее оборудование и, возможно, некоторую легкодоступную информацию. Такие атаки встречаются реже, но носят преднамеренный характер и обычно исходят из внутренних источников. Третий уровень угроз - это крупномасштабные атаки, требующие необычного уровня сложности и оборудования для осуществления атаки.

Атаки третьего уровня обычно исходят из внешнего источника и требуют доступа, физического или виртуального. Атаки третьего уровня крайне редки в современных сетях SAN и могут потребовать значительных знаний и навыков. Ниже приведены три уровня угроз.

Атаки первого уровня являются непреднамеренными и обычно являются результатом обычных ошибок. Классическим примером атаки первого уровня является подключение устройства к неправильному порту. Непреднамеренное подключение может привести к несанкционированному доступу устройства к данным или неправильному форматированию дискового накопителя. Неправильное подключение может даже соединить две сети, что может привести к случайному доступу к сотням портов. Неприятным аспектом этой атаки является то, что она может быть выполнена без особых навыков или размышлений. К счастью, угрозы первого уровня легче всего предотвратить.

Угрозы второго уровня отличаются тем, что кто-то злонамеренно пытается украсть данные или нарушить обслуживание. Разнообразие атак уровня 2 увеличивается по мере того, как злоумышленник (тот, кто инициирует атаку) пытается обойти барьеры. Нарушитель, выдающий себя за авторизованного пользователя, является распространенной атакой уровня 2. Чтобы предотвратить угрозу уровня 2, SAN необходимо добавить процессы и технологии для предотвращения атаки.

Угрозы третьего уровня вызывают наибольшее беспокойство. Это крупномасштабные атаки, которые обычно осуществляются внешним источником с дорогостоящим и сложным оборудованием. Примером такой атаки может быть установка анализатора Fibre Channel, который отслеживает трафик на канале связи. Оборудование для взлома секретов аутентификации или зашифрованных данных - еще один пример атаки третьего уровня. Эти атаки типа "плащ и кинжал" трудновыполнимы и требуют специальных знаний и серьезных намерений для осуществления

атаки. Атаки третьего уровня являются редкими и сложными и выходят за рамки данного технического документа.

Три уровня атак помогают классифицировать угрозы, но для борьбы с каждой из них требуется глубокий анализ. Следующий раздел позволит применить систематический подход к борьбе с отдельными угрозами.

Точки атаки на сеть хранения данных

Угрозы для сетей хранения данных исходят из многих мест. Каждая точка атаки может быть использована как ступенька для последующих атак. Чтобы обеспечить высокий уровень безопасности, между злоумышленником и данными должно быть несколько контрольных точек. Различные точки атаки помогают определить метод защиты для противодействия различным атакам. Подобно тому, как замки имеют несколько защитных механизмов для защиты от захватчиков, предприятие должно установить множество барьеров для предотвращения атак.

Точка атаки помогает в обсуждении отдельных угроз. Угрозы, которые будут обсуждаться в данной работе, включают в себя:

- Несанкционированный доступ
- подмена
- подслушивание

Несанкционированный доступ

Несанкционированный доступ является наиболее распространенной угрозой безопасности, поскольку он может включать в себя все угрозы от 1 до 3 уровня. Несанкционированный доступ может быть простым, как подключение неправильного кабеля, или сложным, как подключение взломанного сервера к сети. Несанкционированный доступ ведет к другим формам атак, и это хорошее место для начала обсуждения угроз.

Доступ можно контролировать в следующих точках атаки:

1. Внеполосное приложение управления - коммутаторы имеют порты Fibre Channel, не относящиеся к Fibre Channel, такие как порт Ethernet и последовательный порт, для целей управления. Физический доступ к порту Ethernet может быть ограничен путем создания частной сети для управления SAN, которая отделена от интранета компании. Если коммутатор подключен к внутренней сети компании, брандмауэры и виртуальные частные сети могут ограничить доступ к порту Ethernet. Доступ к последовательному порту (RS 232) можно ограничить, ограничив физический доступ и обеспечив авторизацию и аутентификацию пользователей. После получения физического доступа к порту Ethernet коммутатор может контролировать приложения, которые могут получить к нему доступ, с помощью списков контроля доступа. Коммутатор также может ограничить приложения или отдельных пользователей, которые могут получить доступ через точку атаки 3.

2. Приложение внутрисетового управления - Еще одна опасность, с которой сталкивается коммутатор, связана с приложением внутрисетового управления. Приложение для внутрисетового управления получает доступ к службам сети, таким как сервер имен и сервер конфигурации сети. Доступ к службам сети контролируется управляющим ACL (MACL).

3. Пользователь к приложению - Как только пользователь получает физический доступ к приложению управления, он должен войти в приложение. Приложение управления может авторизовать пользователя для доступа на основе ролей в зависимости от его должностных функций. Приложение управления должно поддерживать списки контроля доступа и роли для каждого пользователя.

4. Устройство к устройству - После того как два порта Nx_Port вошли в сеть, один порт Nx_port может выполнить вход в порт (PLOGI) другого порта Nx_Port. Зонирование и маскирование LUN могут ограничить доступ устройств на этом этапе. Набор активных зон в каждом коммутаторе будет

обеспечивать ограничения зонирования в Fabric. Устройства хранения данных сохраняют информацию о маскировке LUN.

5. Устройства в Fabric - Когда устройство (Nx_Port) подключается к Fabric (Fx_Port), устройство отправляет команду Fabric Login (FLOGI), содержащую различные параметры, такие как World Wide Name (WWN) порта. Коммутатор может разрешить порту войти в сеть или отклонить FLOGI и разорвать соединение. Коммутатору необходимо поддерживать список контроля доступа (ACL) для WWN, которым разрешено подключение. Реальная угроза для данных возникнет после того, как устройство войдет в сеть, и можно будет перейти к пункту атаки 4 или 5.

6. Коммутатор к коммутатору - Когда коммутатор подключен к другому коммутатору, служба внутреннего соединения (ILS) Exchange Link Parameters (ELP) отправляет соответствующую информацию, например WWN коммутатора. Коммутатор может авторизовать другой коммутатор для формирования более крупной сети или изолировать соединение, если коммутатор не авторизован для присоединения. Каждый коммутатор должен поддерживать ACL для авторизованных коммутаторов.

7. Данные в состоянии покоя - Хранящиеся данные уязвимы к атакам инсайдеров, а также к несанкционированному доступу с помощью атак на основе сети и хостов. Например, поскольку все протоколы хранения являются открытым текстом, администраторы систем хранения, резервного копирования и хостов имеют доступ к хранимым данным в необработанном виде, без ограничений доступа и протоколирования. Устройства шифрования хранилищ обеспечивают уровень защиты данных в состоянии покоя, а в некоторых случаях предоставляют дополнительную аутентификацию и контроль доступа на уровне приложений.

Контроль доступа с помощью списков контроля доступа (ACL) позволяет предотвратить катастрофы. ACL не остановят злоумышленников, которые готовы лгать о своей личности. К сожалению, большинство воров

обычно не возражают против лжи, чтобы получить желаемое. Чтобы предотвратить проникновение в сеть спуферов (тех, кто выдает себя за другого), необходимо также аутентифицировать объект, которому выдается разрешение.

Спуфинг

Подделка - это еще одна угроза, связанная с несанкционированным доступом. Спуфинг имеет множество названий и форм и часто называется: имперсонация, кража личности, угон, маскарад и спуфинг WWN. Спуфинг получает свои названия из-за атак на разных уровнях. Одна форма атаки - выдача себя за пользователя, а другая - маскировка под авторизованный WWN.

Способ предотвращения спуфинга заключается в том, чтобы заставить спуфера предоставить уникальную информацию, которую должен знать только авторизованный пользователь. Для пользователей, информация, которая запрашивается - это пароль. Для устройств секрет связан с WWN порта Nx_Port или коммутатора. Сеансы управления также могут быть аутентифицированы, чтобы убедиться, что злоумышленник не управляет сетью или устройством.

Подделка может быть проверена в следующих точках атаки:

1. Внеполосное приложение управления - Когда приложение управления связывается с коммутатором, коммутатор может проверить подлинность пользователя, который подключается к коммутатору. Аутентификация пользователей рассматривается в пункте атаки 6.

2. Приложение внутриполосного управления - Приложение внутриполосного управления будет использовать аутентификацию Common Transport (CT) для предотвращения подделки команд для Fabric Services.

3. Пользователь к приложению - Когда пользователь входит в приложение, приложение управления запрашивает у пользователя пароль,

секрет или пропуск. Приложение может аутентифицировать пользователя с помощью биометрических данных, таких как отпечатки пальцев, сканирование сетчатки глаза или даже образцы ДНК.

4. Устройство к устройству - После того как Nx_порт получает PLOGI, Nx_порт может запросить запрашивающий порт предъявить свои учетные данные. CHAP является стандартным механизмом Fibre Channel для аутентификации Nx_Port. Запрашивающий Nx_Port должен также запросить другой Nx_Port, чтобы оба порта были уверены в подлинности другого порта. Двусторонняя аутентификация известна как взаимная аутентификация.

5. Устройства к Fabric - Когда устройство отправляет команду Fabric Login (FLOGI), коммутатор может ответить запросом CHAP для аутентификации пользователя. Порт Nx_Port должен ответить на CHAP и запросить коммутатор для взаимной аутентификации.

6. Switch to Switch - Когда коммутатор подключен к другому коммутатору, оба коммутатора должны аутентифицировать друг друга с помощью CHAP.

Для аутентификации каждой точки возможны четыре типа аутентификации:

1. Аутентификация пользователя
2. Аутентификация объекта Ethernet CHAP
3. Аутентификация сообщений CT
4. Fibre Channel DH-CHAP Аутентификация сущности

После того как объекты и пользователи авторизованы и аутентифицированы, трафик должен безопасно передаваться между авторизованными устройствами. Данные, проходящие по каналу связи, все еще могут быть украдены сниффером. Снифферы будут рассмотрены в последней угрозе.

Сниффинг

Данные могут быть украдены различными способами. Одним из способов кражи данных является их перехват во время полета. Обнюхивание также называют прослушкой и является одной из форм атаки "человек посередине". Анализатор Fibre Channel является хорошим примером сниффера, который может прозрачно отслеживать трафик. При правильном выполнении сниффинг не влияет на работу устройств на канале связи. Лекарством от сниффинга является шифрование.

Шифрование - это процесс получения необработанных данных и их зашифровки таким образом, что они не могут быть прочитаны без правильного секрета. Без правильного ключа украденные данные ничего не стоят. Существует несколько методов шифрования, и для разных видов трафика существуют разные алгоритмы шифрования. Вместо того, чтобы обсуждать методы шифрования для каждой точки атаки, метод шифрования применяется только к внутрисполосному и внеполосному трафику.

Encapsulating Security Payload (ESP) может шифровать трафик Fibre Channel для обеспечения конфиденциальности. Трафик Ethernet может быть зашифрован с помощью Secure Sockets Layer (SSL) или аналогичных протоколов. Эти методы шифрования могут использовать различные уровни шифрования, чтобы сделать украденные данные бесполезными.

Таким образом, угрозы, которые может реализовать злоумышленник:

- Несанкционированный доступ;
- Сниффинг;
- Спуффинг.

Точки атаки:

- Приложения;
- Сетевое оборудование;

- Диски.

Что мониторить: сетевое оборудование и диски. Надо смотреть попытки авторизации, обмена информацией между устройствами. Как указано выше, есть шесть позиций, на которых можно ограничить доступ, каждый из этих рубежей можно мониторить.

Коды:

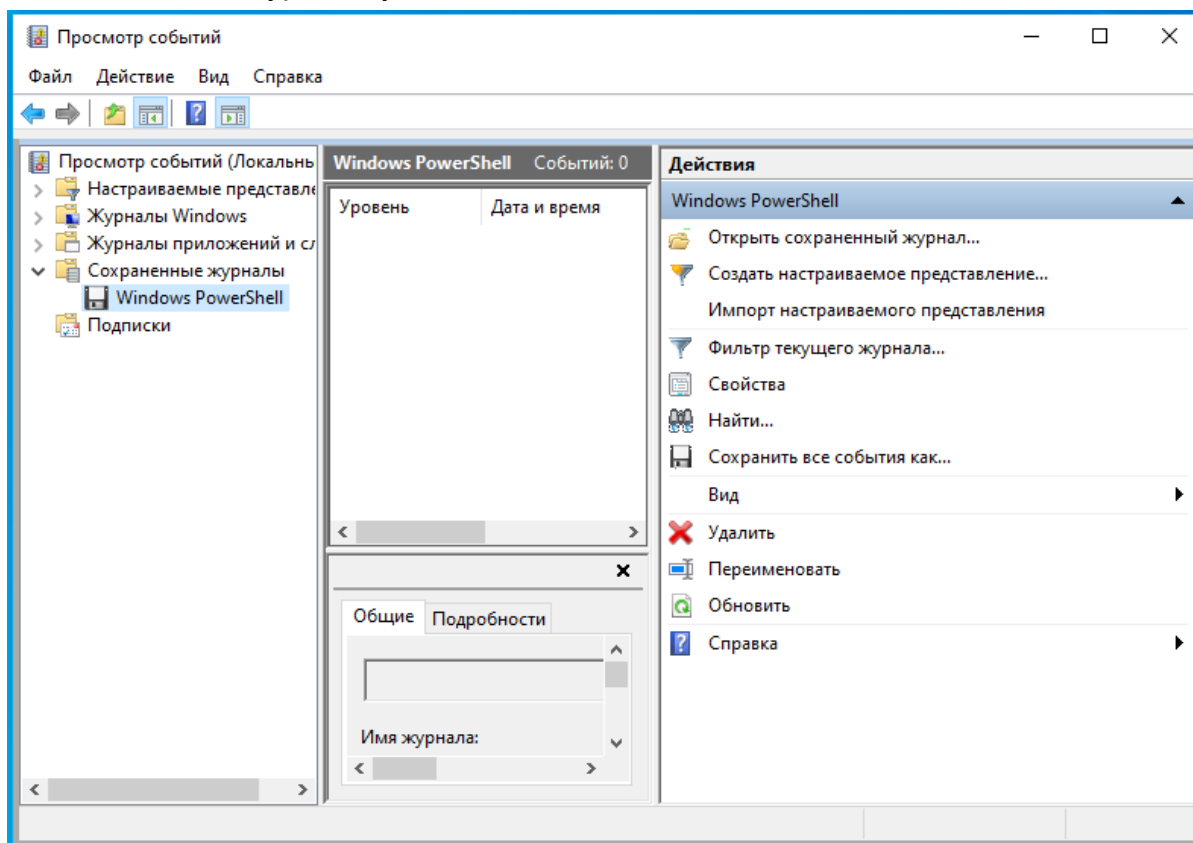
- 21 - A Gateway processor memory fault was detected.
- 25 - A Gateway PCI bus parity error was detected.
- 26 - A Gateway PCI interface error was detected
- 33 - An interface has detected a bus fault (event message indicates the specific interface)
- 34 - An interface has detected a device fault (event message indicates the specific interface).
- 41 - A Fibre Channel transfer failure has occurred. Note: Error recovery may have succeeded.
- 59, 60 - power has entered alarm change
- 100 - power supply is out of specification
- 106 - Fibre Channel interface failed the health check

Часть 2. Журналирование событий в ОС Windows.

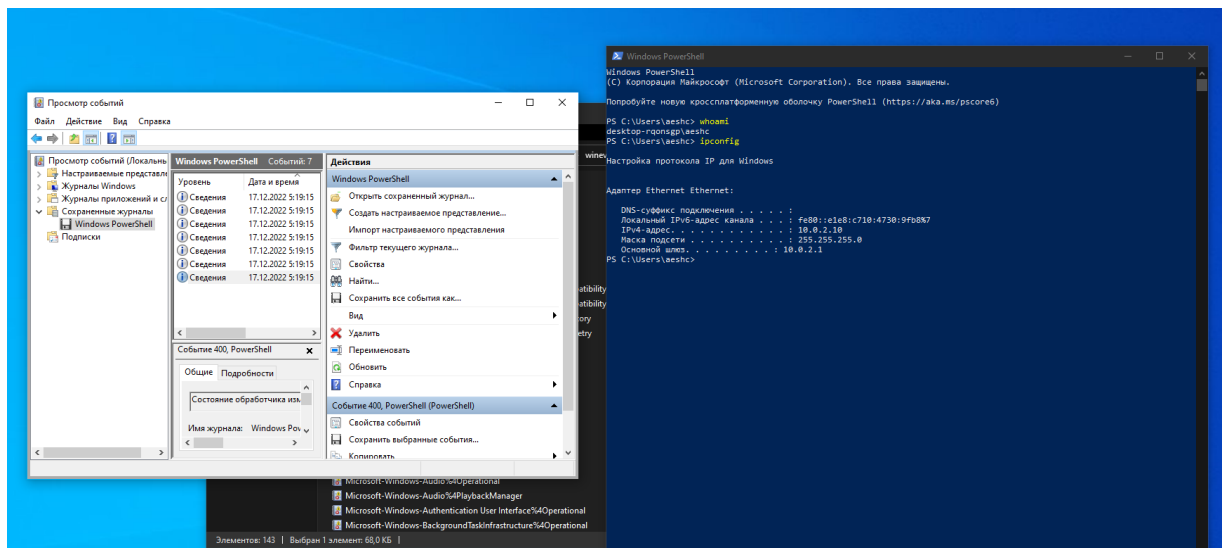
Задание 1. PowerShell.

Журнал событий C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx.








Виртуальная машина установлена новая, никаких действий не производилось, следовательно, журнал пустой.



В консоли PowerShell выполнены 2 команды: `whoami` и `ipconfig`, в связи с чем в журнале событий появились 7 событий.



Windows PowerShell Событий: 7

Уровень	Дата и время	Источ...	Код со...	Категор...
 Сведения	17.12.2022 5:19:15	PowerS...	600	Жизне...
 Сведения	17.12.2022 5:19:15	PowerS...	600	Жизне...
 Сведения	17.12.2022 5:19:15	PowerS...	600	Жизне...
 Сведения	17.12.2022 5:19:15	PowerS...	600	Жизне...
 Сведения	17.12.2022 5:19:15	PowerS...	600	Жизне...
 Сведения	17.12.2022 5:19:15	PowerS...	600	Жизне...
 Сведения	17.12.2022 5:19:15	PowerS...	400	Жизне...

Событие 600, PowerShell (PowerShell)

Общие Подробности

Поставщик "Registry" находится в состоянии Started.

Подробные сведения:
ProviderName=Registry
NewProviderState=Started

SequenceNumber=1
HostName= ConsoleHost

Имя журнала: Windows PowerShell

Источник: PowerShell (PowerShell) Дата: 17.12.2022 5:19:15

Код 600 Категория задачи: Жизненный цикл поставщика

Уровень: Сведения Ключевые слова: Классический

Пользов.: Н/Д Компьютер: DESKTOP-RQONSGP

Код операции: Сведения

Подробности: [Справка в Интернете для](#)

Поставщик "Alias" находится в состоянии Started.

Поставщик "Environment" находится в состоянии Started.

А также FileSystem, Variable, Function.

При повторном выполнении команд в консоли новых событий не появляется, следовательно, вышеперечисленные события связаны с включением консоли и настройкой "поставщиков" (окружения?).

предположение подтверждается выключением и повторным включением консоли - прибавились такие же 7 событий.

Где найти логи о выполнении команд в power shell - не знаем.

Журнал команд можно посмотреть через саму консоль командой get-history, но она стирается при перезапуске сессии.

```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\aeshc> Get-history
PS C:\Users\aeshc> whoami
desktop-rqonsgp\aeshc
PS C:\Users\aeshc> ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::e1e8:c710:4730:9fb8%7
    IPv4-адрес. . . . . : 10.0.2.10
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 10.0.2.1
PS C:\Users\aeshc> ping 10.0.2.9

Обмен пакетами с 10.0.2.9 по с 32 байтами данных:
Ответ от 10.0.2.9: число байт=32 время<1мс TTL=64
Ответ от 10.0.2.9: число байт=32 время<1мс TTL=64
Ответ от 10.0.2.9: число байт=32 время<1мс TTL=64
Ответ от 10.0.2.9: число байт=32 время<1мс TTL=64

Статистика Ping для 10.0.2.9:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\Users\aeshc> Get-history



Id CommandLine
--
1 Get-history
2 whoami
3 ipconfig
4 ping 10.0.2.9


PS C:\Users\aeshc> 
```

Задание 2. Касперский.

После скачивания вредоносной программы быстрая проверка обнаружила угрозы и предложила их устранить. При попытке запустить вредоносную программу антивирус заблокировал это действие.

Защита

	C:\ProgramData\KMSAutoS\KMSAuto Net.exe Обнаружена вредоносная утилита. Время: 16.09.2022 19:38	Устранить ▼
	C:\Users\aeshe\Downloads\k... 2016 v1.5.4 Portable\KMSAuto Net.exe Обнаружена вредоносная утилита. Время: 17.09.2022 5:28	Устранить ▼

 Сегодня, 17.09.2022 5:29:25 Процесс завершен

Событие: Процесс завершен
Программа: KMSAuto Net
Пользователь: DESKTOP-RGKF4BA\aeshe
Тип пользователя: Активный пользователь
Компонент: Мониторинг активности
Описание результата: Завершен
Тип: Упакованная программа, которая может нанести вред
Название: not-a-virus:PDM:HackTool.Win32.Yzon.a
Степень угрозы: Средняя
Тип объекта: Процесс

Первый файл успешно вылечен антивирусом без помещения в карантин, второй добавлен в исключения.

Обнаружено: HackTool.MSILHackKMS.gen
Расположение: C:\Users\ae...Portable\KMSAuto Net.exe

Не удается вылечить обнаруженный объект.

Удалить

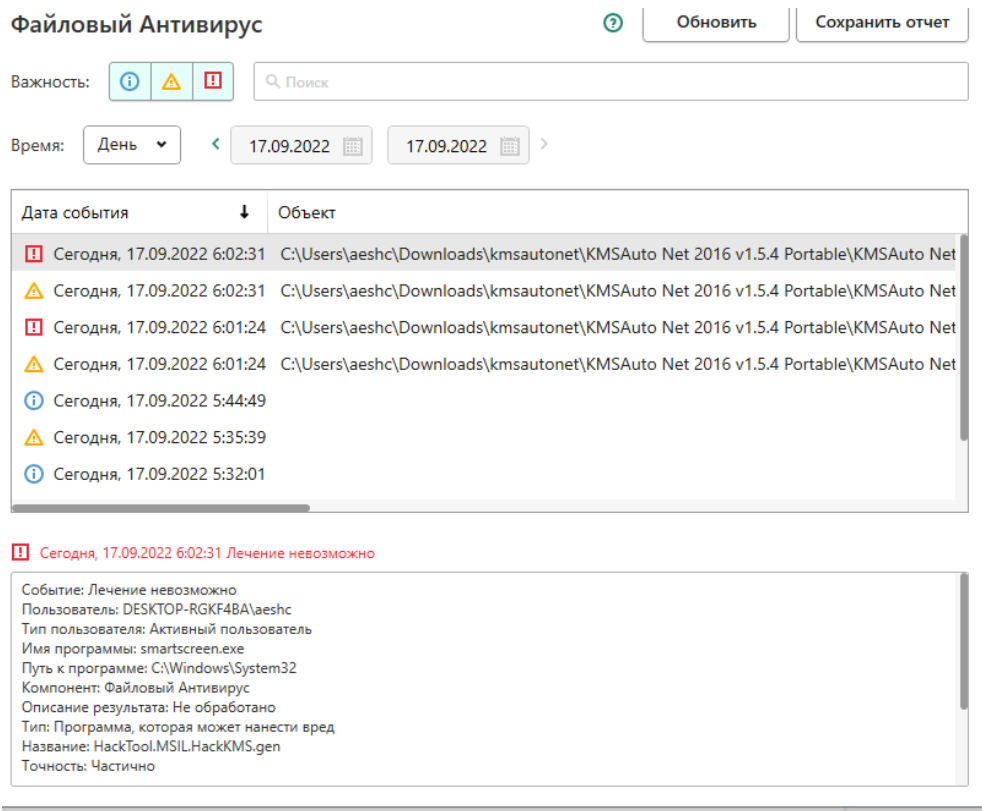
Пропустить

Добавить в исключения

Логи установки или удаления программ хранятся в папке %USERPROFILE%\AppData\Local\Temp

В ней обнаружена папка пустая Temp1_kmsautonet.zip\kmsautonet.

Журнал событий обычный:



Журнал событий в текстовом виде:

Сегодня, 17.09.2022 6:02:31 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net.exe KMSAuto Net.exe
C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable Файл
Не обработано Лечение невозможно Не обработано
HackTool.MSIL.HackKMS.genПрограмма, которая может нанести вред
Средняя Частично Windows Defender SmartScreen smartscreen.exe
C:\Windows\System32\smartscreen.exe C:\Windows\System32 9284
DESKTOP-RGKF4BA\aeshe Активный пользовательПропущено
Сегодня, 17.09.2022 6:02:31 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net.exe KMSAuto Net.exe
C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable Файл
Обнаружено Обнаружена легальная программа, которая может
быть использована злоумышленником для нанесения вреда компьютеру или
данным пользователя Обнаружено HackTool.MSIL.HackKMS.gen
Программа, которая может нанести вред Средняя Частично Windows
Defender SmartScreen smartscreen.exe
C:\Windows\System32\smartscreen.exe C:\Windows\System32 9284
DESKTOP-RGKF4BA\aeshe Активный пользователь Экспертный анализ
Сегодня, 17.09.2022 6:01:24 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto

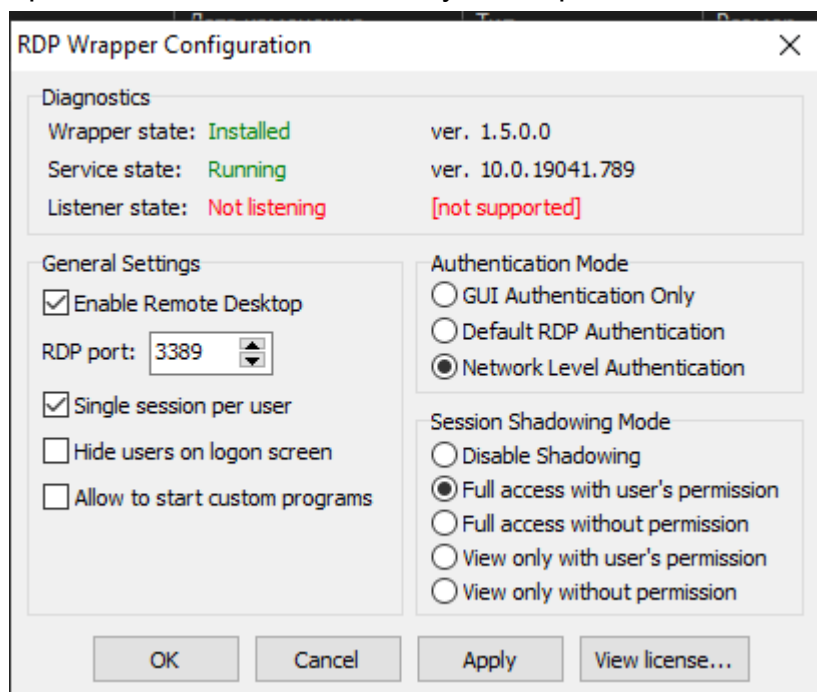
Логи о помещении файлов в карантин хранятся в другом файле:
C:\ProgramData\Kaspersky Lab\AVP21.3\SysWHist

Выводы:

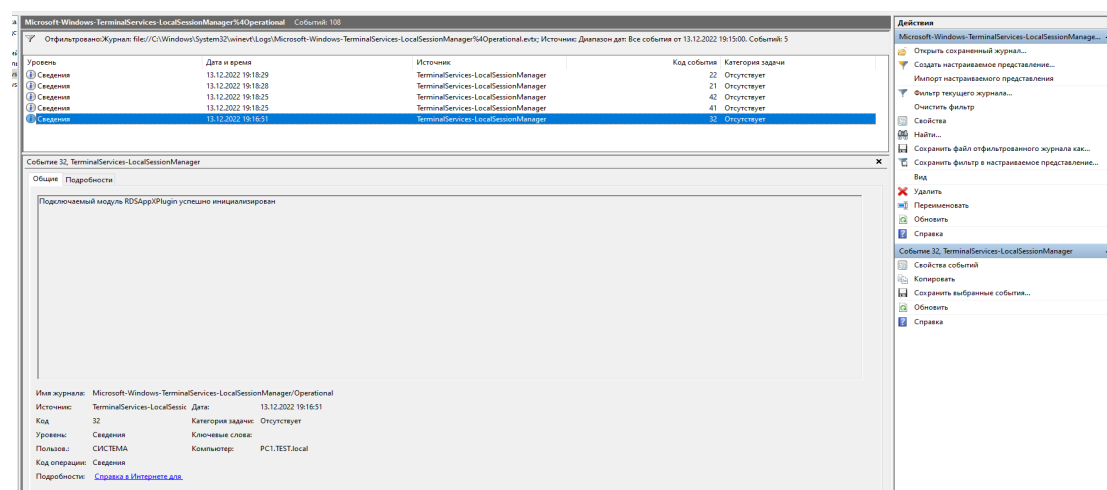
- информация о добавлении вируса в исключения не записана в журнале, это можно посмотреть только в самой вкладке “исключения”
- о том, что вирус найден, запись лога есть, можно увидеть пользователя, ее скачавшего или запустившего

Задание 3. RDP.

Пришлось повозиться, потому что версия винды - home, а не pro.



Подключились по RDP к этой машине с другой виртуалки.

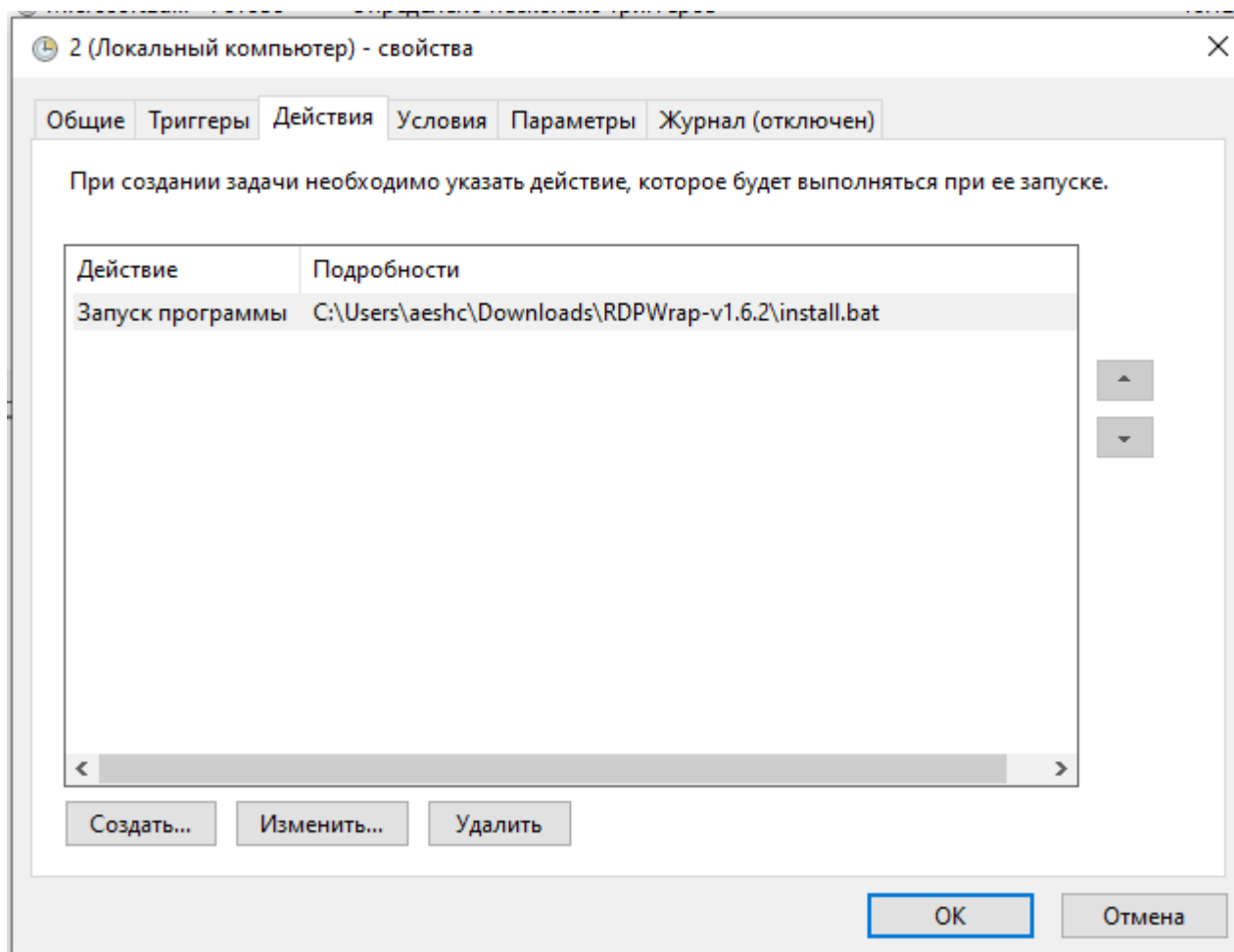


Остальные события аналогично: подключаемый модуль RDP инициализирован, начать/завершить разрешение спора для сеанса с пользователем aeshcherbakova

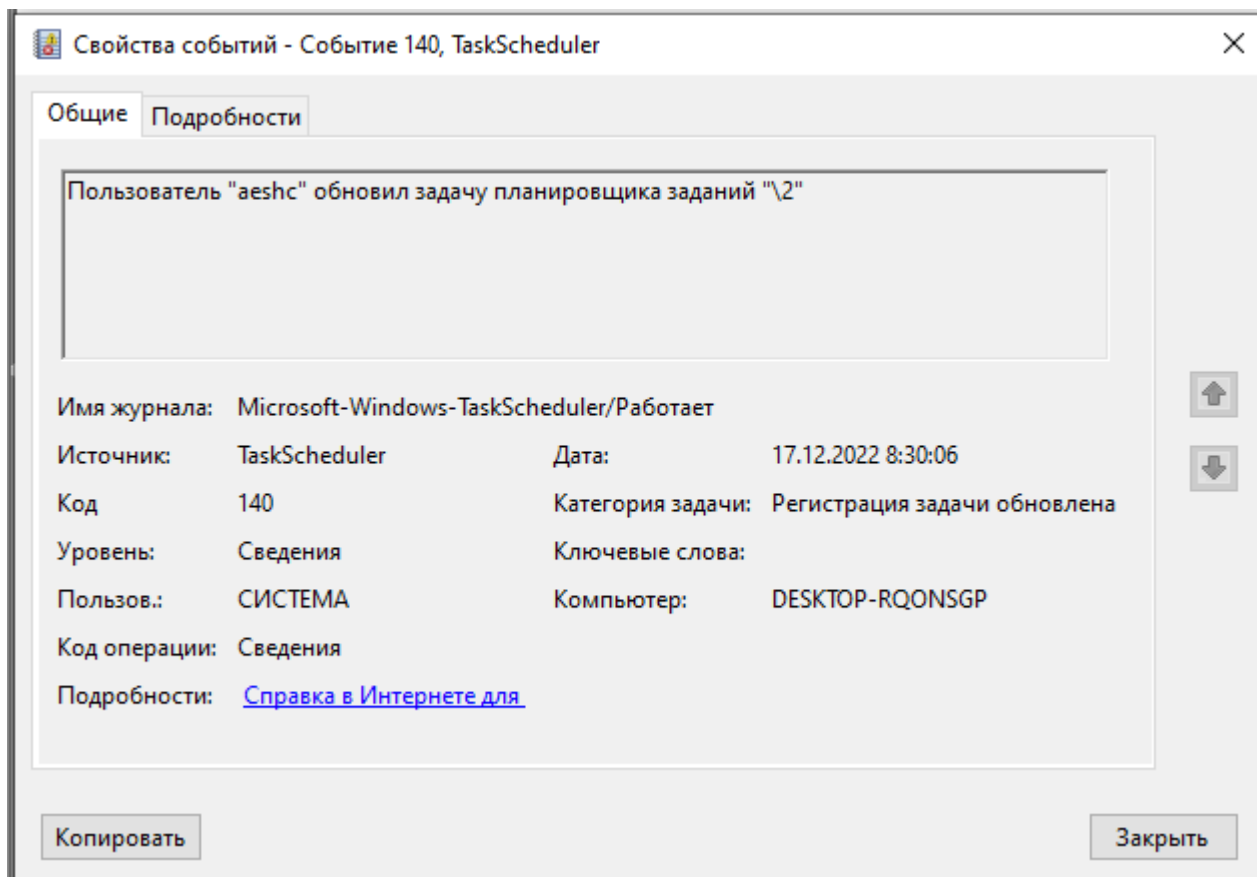
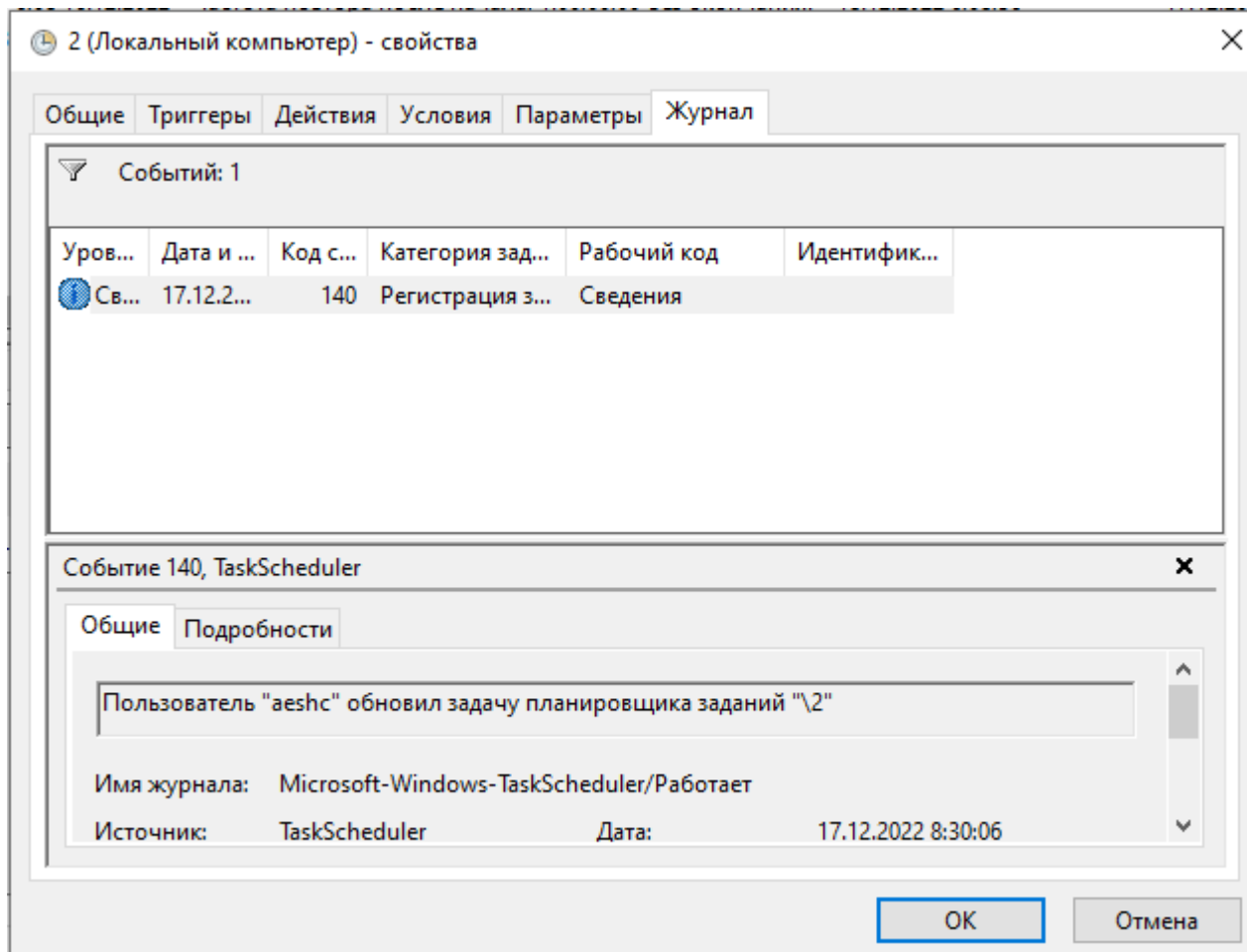
Информация из логов: какой пользователь подключается, время, успешно/неуспешно.

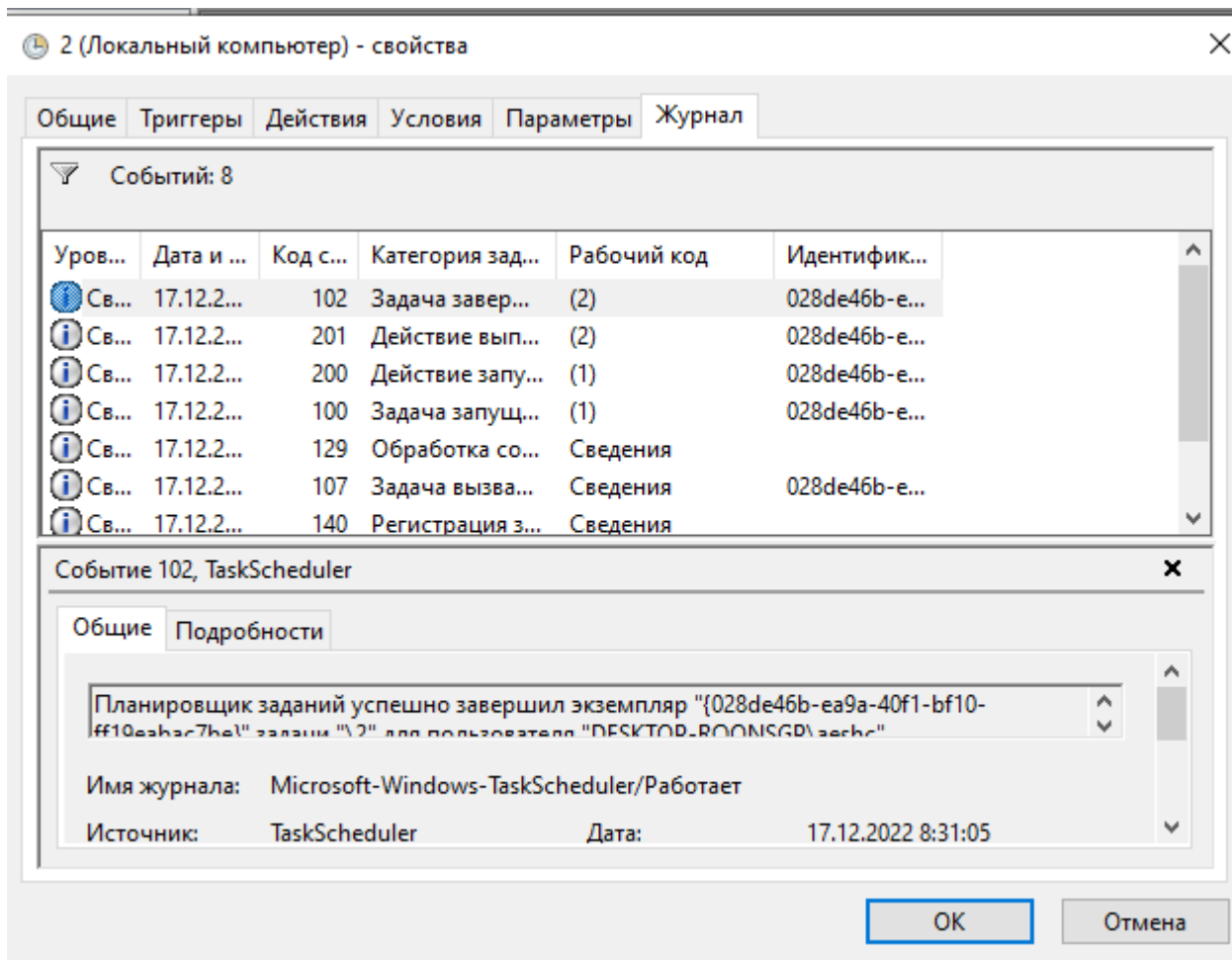
Задание 4. Планировщик задач.

Создана простая задача на запуск программы в определенное время. Отработала корректно.



Файл	Состояние	Триггеры	Время следующего запуска	Время прошлого запуска	Результат последнего запуска	Автор	Создан
1	Готово	В 8:18 17.12.2022		30.11.1999 0:00:00	Это задание еще не выполнялось. (0x41303)	DESKTOP-RQONSGP\aeshe	17.12.2022
2	Готово	В 8:21 17.12.2022		17.12.2022 8:21:43	Операция успешно завершена. (0x0)	DESKTOP-RQONSGP\aeshe	17.12.2022





Получилось включить журнал для задач. Задача отработала повторно, логи есть, но только во вкладке “журнал” этой самой задачи. В общий журнал (Microsoft-Windows-TaskScheduler%4Maintenance) логи не занеслись. Почему - неизвестно.

